21 CFR PART 11

IMPLEMENTATION GUIDE

OptiZeus SCADA · Version 2.5.4

Document: CFR11-OZ-SCADA ·

WHAT IS 21 CFR PART 11?

21 CFR Part 11 is an **FDA regulation** defining criteria under which electronic records and electronic signatures are considered trustworthy and equivalent to paper records. It applies to all FDA-regulated industries: pharmaceutical, biotech, medical device, and food manufacturing.

OptiZeus SCADA fully satisfies **Subpart B (Electronic Records §11.10)** and **Subpart C (Electronic Signatures §11.50–§11.300)**. This document maps every regulatory paragraph to the specific OptiZeus feature that fulfils it.

APPLICABLE RECORDS IN OPTIZEUS

Batch Records
Execution data, parameters, operator actions

Alarm Journal
Alarms raised, acknowledged, time-stamped

Audit Trail
Every config change and control action

Electronic Signatures
Batch close, recipe approval, overrides

Process Historian
Tag values from PLCs and instruments

User Access Logs
Logins, logouts, failed attempts

Config Records
System configuration before/after values

Calibration Events
Equipment calibration records via OPC UA

REGULATION STRUCTURE

Subpart B — Electronic Records

- ✓ §11.10 Controls for closed systems (a)–(k)
- ✓ §11.30 Controls for open systems

Subpart C — Electronic Signatures

- ✓ §11.50 Signature manifestations
- ✓ §11.70 Signature / record linking
- ✓ §11.100 General requirements
- ✓ §11.200 Electronic sig. components
- ✓ §11.300 Controls for ID codes & passwords

OVERALL COMPLIANCE STATUS

§11.10	Electronic Records Controls	COMPLIANT
§11.30	Open Systems Controls	COMPLIANT
§11.50	Signature Manifestations	COMPLIANT
§11.70	Sig. / Record Linking	COMPLIANT
§11.100	General Sig. Requirements	COMPLIANT
§11.200	Sig. Components & Controls	COMPLIANT
§11.300	ID & Password Controls	COMPLIANT

§ Ref	Requirement	OptiZeus Implementation — Key Points	Status
§11.10(a)	System Validation	• GAMP5 Cat.4 package auto-generated: URS, FS, DS, IQ, OQ, PQ, TM, VSR • Full test protocols with acceptance criteria per qualification phase • Annual revalidation cycle — triggered on any software update	COMPLIANT
§11.10(b)	Legible Record Copies	• PDF export: audit trail, batch records, historian trends, alarm journal • CSV / Excel export for electronic submission to regulators • All exports include timestamp, system version, and user identity	COMPLIANT
§11.10(c)	Record Protection	• SQL Server append-only audit table — no user can DELETE records • Role-based access: Viewer cannot access configuration data • Automated backup with tested restore — configurable retention period	COMPLIANT
§11.10(d)	Authorised Access	• Unique username + bcrypt-hashed password per individual — no shared accounts • MFA / TOTP second factor mandatory for Admin and Engineer roles • 5-level RBAC enforced server-side on every API request	COMPLIANT
§11.10(e)	Computer-Generated Audit Trail	• Every action logged: user, UTC timestamp, IP, action type, old/new value • Covers tag writes, alarm acks, config changes, logins, batch events • Append-only SQL Server table — immutable by design, no delete permission	COMPLIANT
§11.10(f)	Operational Sequence Checks	• ISA-88 batch engine enforces phase order — steps cannot be skipped • Recipe requires QA-approved sign-off before production execution • E-signature gate required before each critical batch operation	COMPLIANT
§11.10(g)	Authority Checks	• All RBAC checks performed server-side — zero client-side trust • E-signature: password re-entered at the moment of signing • Batch close requires minimum Supervisor role — enforced by API	COMPLIANT
§11.10(h)	Device / Input Checks	• Every API endpoint validates input type, range, and format • OPC UA Bad-quality tags flagged in HMI and excluded from batch records • Out-of-range tag writes rejected with alarm — logged in audit trail	COMPLIANT
§11.10(i)	Training & Education	• User accounts include: role, department, training date fields • GAMP5 URS / FS documents operator training as a mandatory requirement • Zeus Automation provides role-specific training documentation per tier	COMPLIANT
§11.10(j)	Accountability Policies	• SOP templates provided: e-signature policy and user account management • Every e-signature records: user ID, timestamp, declared meaning (reason code) • SHA-256 cryptographic hash links signature to exact record — non-repudiation	COMPLIANT
§11.10(k)	Documentation Controls	• GAMP5 document suite version-controlled with approval workflow • Config changes only via Test→Production workflow with QA sign-off • Full change log maintained — every deployment audited and traceable	COMPLIANT

SUBPART C — ELECTRONIC SIGNATURES COMPLIANCE

§11.50(a) Signature Manifestation — COMPLIANT

- Every e-sig stores: full name, UTC timestamp, reason code
- Reason codes: Approve / Review / Verify / Batch-Close / Override
- Displayed on audit PDF and batch record exports

§11.70 Signature–Record Linking — COMPLIANT

- SHA-256 hash over: record + timestamp + user ID + reason code
- Hash stored with signature — any record change invalidates it
- Verification routine runs on every audit record retrieval

§11.100(a) Unique Sig. Per Individual — COMPLIANT

- Username unique at DB level (UNIQUE constraint) — never reassigned
- Departed users: account disabled not deleted — full history preserved
- LDAP/AD enforces enterprise-wide uniqueness

§11.100(b) Identity Verification — COMPLIANT

- New accounts require admin creation with documented identity check
- First-login mandatory password change enforced by system
- Training record and role assignment documented in GAMP5 URS

§11.200(a) Two-Component Signatures — COMPLIANT

- Component 1: unique username · Component 2: bcrypt password
- Optional Component 3: MFA/TOTP (mandatory for Admin/Engineer)
- Password re-entry required at point of signing — not just login

§11.300(a) Unique ID + Password — COMPLIANT

- Username uniqueness enforced at database level
- Cannot reuse last 5 passwords (configurable)
- LDAP/AD enforces enterprise password complexity rules

§11.300(b) Periodic Credential Review — COMPLIANT

- Password expiry: configurable — default 90 days
- Admin console flags accounts inactive >60 days for review
- LDAP sync automatically disables departed employee accounts

§11.300(c) Revocation of Compromised Cr — COMPLIANT

- Admin disables any account instantly from the management console
- All active sessions for disabled user terminated immediately
- Account disable event recorded in audit trail with admin user + timestamp

AUDIT TRAIL — RECORD STRUCTURE (Append-Only · No Delete for Any Role)

Record ID	Auto-increment unique key — immutable primar	**Timestamp**	Server UTC — cannot be manipulated by client
Username	Authenticated user ID at time of action	**Display Name**	Full name of operator for human-readable export
IP Address	Client IP — detects shared/remote access sessi	**Session ID**	Links all actions within one login session
Action Type	TAG_WRITE / ALARM_ACK / CONFIG_CHANGE / LOGIN /	**Target Object**	Tag name, alarm ID, screen name, or user account
Old Value	Value before the change was applied	**New Value**	Value after the change was applied
Reason Code	E-sig reason: APPROVE / REVIEW / VERIFY / BATCH_CLOSE	**SignatureHash**	SHA-256 — cryptographically binds signature to rec

ROLE-BASED ACCESS CONTROL (5 Levels — Enforced Server-Side on Every API Call)

ADMINISTRATOR

- Full system configuration access
- User account create / disable
- Read-only access to audit trail
- Cannot delete any audit record
- License and server management

ENGINEER

- Tag database configuration
- HMI screen design and deploy
- Alarm rules and threshold config
- Recipe and batch template creation
- Protocol driver configuration

SUPERVISOR

- Alarm acknowledgement and shelving
- Batch start / pause / abort / close
- E-signature on critical operations
- Override alarm limits (with e-sig)
- Report generation and approval

OPERATOR

- HMI screen monitoring and control
- Tag write within configured limits
- Standard alarm acknowledgement
- Batch step execution
- Personal shift report viewing

VIEWER

- Read-only HMI monitoring only
- Alarm viewing — no acknowledgement
- Historian trend chart viewing
- No write operations of any kind
- No access to audit trail

PART 11 CONFIGURATION CHECKLIST

USER MANAGEMENT

- ☐ Unique username per individual — no shared accounts
- ☐ Password policy: min length, complexity, 90-day expiry
- ☐ MFA / TOTP enabled for Admin and Engineer roles
- ☐ Auto-logout timeout configured per role
- ☐ LDAP / AD integration configured and tested
- ☐ User departure procedure: immediate account disable
- ☐ Annual access rights review scheduled

AUDIT TRAIL

- ☐ Audit trail enabled — writing to SQL Server (not SQLite)
- ☐ Confirmed: no user has DELETE on audit table
- ☐ Audit trail PDF and CSV export tested successfully
- ☐ Retention policy defined, documented, and enforced
- ☐ Audit trail included in scheduled backup
- ☐ Quarterly audit trail review scheduled in SOP

ELECTRONIC SIGNATURES

- ☐ E-signature enabled: batch close operation
- ☐ E-signature enabled: recipe approval workflow
- ☐ E-signature enabled: critical tag overrides
- ☐ Password re-entry at signing confirmed (not just login)
- ☐ Reason code list reviewed and approved by QA
- ☐ SHA-256 signature hash verification tested

SYSTEM & DATA INTEGRITY

- ☐ HTTPS / TLS certificate installed and browser-validated
- ☐ SQL Server configured for production — not SQLite
- ☐ Database backup schedule configured and restore tested
- ☐ System clock synchronised to NTP server
- ☐ Store & Forward tested — data preserved during outage
- ☐ Disaster recovery procedure documented and rehearsed

REQUIRED SOPs FOR PART 11 COMPLIANCE

SOP-001 User Account Management
- New account creation and identity verification process
- Role assignment based on documented job function
- User departure — immediate account disable procedure
- Annual access rights review and documentation
- Shared account prohibition policy

SOP-002 Electronic Signature Policy
- Conditions requiring an electronic signature
- Defined meaning of each reason code
- Password security obligations per user
- Reporting procedure for compromised credentials
- Non-repudiation statement acknowledgement

SOP-003 Audit Trail Review
- Review frequency — minimum quarterly
- Scope and sampling methodology
- Escalation path for anomalous entries
- Annual comprehensive full-scope review
- Archival and retention of review records

SOP-004 System Change Control
- Change request initiation and approval workflow
- Impact classification: Minor / Moderate / Major
- Testing requirements based on impact level
- Documentation update requirements per change
- QA sign-off gate required before go-live

SOP-005 Backup & Disaster Recovery
- Backup schedule, media type, and storage location
- Restore testing frequency and acceptance criteria
- Recovery time objective (RTO) and RPO targets
- Offsite / cloud backup requirements

SOP-006 Periodic System Review
- Annual review scope, checklist, and sign-off
- Regression test suite execution requirements
- User access rights annual audit procedure
- Revalidation trigger criteria and decision tree

21 CFR PART 11 — IMPLEMENTATION SIGN-OFF

By signing, the undersigned confirm OptiZeus SCADA is configured and operating in compliance with 21 CFR Part 11.

ROLE / TITLE	PRINTED NAME	SIGNATURE	DATE
Quality Assurance Manager			
Validation Manager			
System Owner / IT Manager			
Zeus Automation Representative			

CFR11-OZ-SCADA · optizeus.org · zeus-automation.com · sales@optizeus.org